

said subset of rules comprising a second rule, which specifies second header information, and a second subset of rules, said second subset of rules relating to said second rule,

~~processing a data packet according to a rule belonging to the set of rules, the header information of said data packet matching the header information of said rule.~~

~~- in said step of comparing a data packet, comparing said data packet is compared to said second subset of rules only if the header information of the data packet matches the header information of the said second rule.~~

15. [currently amended] A computer readable medium having stored thereon a data structure comprising:

screening information fields, wherein said screening information stored in said screening information fields is hierarchically structured so that it comprises a first rule, which specifies first header information, and a subset of rules relating to said first rule, said first header information being common to said rules belonging to said subset of rules, and wherein at least one rule belonging to said subset of rules comprises a generic information portion, said generic information portion to be replaced with second information before a data packet is compared to said at least one rule.

Both of claims 2 and 15 are now directed to statutory subject matter. Claim 2 is a process. Claim 15 is a data structure now because it now has been amended to specify a computer readable medium having stored thereon screening information fields.

Claims 1-6 and 13-17 were rejected for obviousness over Ke et al. (PCT US00/08708) in view of Coss (EP 0909075 A1).

PATENT

Claims 1 and 17 have been cancelled. With regard to this obviousness rejection as applied to the remaining claims, please consider the following with respect to this rejection. Ke et al. discloses a gateway for screening packets transferred over a network. The gateway includes a plurality of network interfaces, a memory and a memory controller. Each network interface receives and forwards messages from a network through the gateway. The memory temporarily stores packet received from a network. The memory controller couples each of the network interfaces and is configured to coordinate the transfer of received packets to and from the memory using a memory bus. The gateway includes a firewall engine implemented in a hardware ASIC and coupled to the memory bus.

The ASIC includes an internal rule memory for storing one or more rule sets used by the firewall engine for screening packets. The internal rule memory includes often accessed rule sets while the external rule memory is configured to store lesser accessed rule sets. The internal rule memory includes a first portion of a rule set, and a second portion of the rule set is stored in the external rule memory.

Thus, in Ke et al., a performance bottleneck caused by the retrieval of rules from the external memory over the memory bus is alleviated by means of storing the frequently used rules (a first set of rules) in an internal rule memory of the firewall engine. The relatively rarely used rules (a second set of rules) are stored into the external memory.

Therefore, Ke et al. fails to teach or suggest screening information comprising a set of rules which are hierarchically arranged so as to comprise a first rule which specifies first header information and a subset of rules relating to the first rule.

The Examiner refers, in support of the obviousness rejection, to page 3, lines 30-33 in Ke et al.: "The internal rule memory includes oft accessed rule sets while the external rule memory is configured to store lesser accessed rule sets. The internal rule memory

includes a first portion of a rule set, and a second portion of the rule set is stored in the external rule memory.

The above quoted section of Ke et al. only teaches that the rules are stored in different memories according to their expected frequency of use. The "second port of a rule set" is not a hierarchical subset of the "first portion of a rule set" as is the case in the claimed invention.

Further, Ke et al. fails to teach or suggest comparing a data packet to said subset of rules only if the header information of the data packet matches the header information of the first rule. This is a significant feature of the claimed invention as it saves time to not have to check rules in the subset if the first rule is not satisfied.

The Examiner refers to page 8, lines 9-21 in Ke et al. This section of Ke et al. merely describes examples of contents of the rules. This section does not make any description of searching matching rules, i.e., comparing a data packet to the rules. More particularly, this section of Ke et al. fails to teach or suggest comparing a data packet to said subset of rules only if the header information of the data packet matches the header information of the first rule.

Also, the Examiner admits that Ke et al. fails to teach or suggest the hierarchically structured screening information as claimed in the amended claims submitted herewith. To supply this feature, the Examiner refers to Coss. Coss discloses a computer network firewall that can be configured to cache the rule processing results for one or more packets, and then utilize the cached results to bypass rule processing for subsequent similar packets. For example, the results of applying a rule set to a particular packet of a network session may be cached, such that when a subsequent packet from the same network session arrives in the firewall, the cached results from the previous packet are used for the subsequent packet. This avoids the need to apply the rule set to each

incoming packet.

The Examiner refers to page 7, lines 45-50, and Figure 8 in Coss. This section of Coss merely teaches that a session may include a connection also in a reverse direction (e.g., back to the user). A hit count, i.e., a predetermined number of matches, has to be accumulated prior to selection of a rule for action for the reverse connection. This section has nothing to do with hierarchically arranged screening information as claimed in the present invention.

Therefore, the claimed invention is patentable over Ke et al. in view of Coss because, even if the two references were combined, the knowledge needed to make the claimed invention would still be missing. Neither reference teaches hierarchically arranged rule sets and not checking a subset of rules if there is no match between the header of a packet to be tested and first header information in a first rule. This saves time and is a key feature of the invention which is not found in the prior art. **The Court of Appeals for the Federal Circuit has held that for the prima facie case obviousness to exist based upon a combination of references, the prior art itself must suggest to those skilled in the art that they should make the combination, and the prior art (and not the applicant's disclosure) must contain teachings that would lead one of ordinary skill in the art to have a reasonable expectation of success. In re Vaeck, 947 F.2d 488 [20 USPQ2d 1438] (Fed. Cir. 1991).** Both suggestion and reasonable expectation of success must be found in the prior art and not in the applicant's specification. *Id.* Where the prior art does not contain all the knowledge needed to solve the problem and does not even recognize the problem, it is unlikely that the Federal Circuit would find that a reasonable expectation of success could be found in the prior art itself and the invention cannot rightfully be called obvious.

Here, the prior art does not contain the hierarchical data structure of the rule set nor the threshold comparison of the header to the first rule and skipping checks against the subset if the first rule is not met.

Regarding new claim 18, Ke et al. and Coss do not teach or suggest the following feature:

and wherein said screening information comprises a first part, which is modifiable by an entity authorized to configure said gateway element, and a second part, which is modifiable by an entity specifically authorized to modify said second part.

Accordingly, claim 18 is not obvious since the combination of the prior art does not contain all the knowledge needed to make the invention, so one skilled in the art would not perceive a likelihood of success in solving the problem the inventor solved by combining the two references.

Regarding new claim 19, Ke et al. and Coss do not teach or suggest the following feature:

and wherein said screening information comprises a first part, which is modifiable by an entity authorized to configure said gateway element, and a second part, which is modifiable by an entity specifically authorized to modify said second part.

Accordingly, claim 19 is not obvious since the combination of the prior art does not contain all the knowledge needed to make the invention, so one skilled in the art would not perceive a likelihood of success in solving the problem the inventor solved by combining the two references.

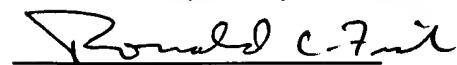
Since neither Ke et al. nor Coss teach or suggest all the features of the independent claims, they also fail to teach or suggest the features of the dependent claims. Therefore, all the claims are believed to be in condition for allowance.

PATENT

July 13, 2005

Respectfully submitted,

Dated: July 14, 2005

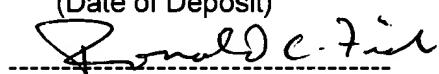


Ronald Craig Fish
Reg. No. 28,843
Tel 408 866 4777
FAX 408 866 4785

I hereby certify that this correspondence is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to: Commissioner for Patents , P.O. Box 1450, Alexandria, Va. 22313-1450.

on 7/14/05

(Date of Deposit)


RONALD CRAIG FISH